TITLE OF THE INVENTION

A system for anonymous distribution and delivery of digital goods.

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is related to and claims priority from U.S. Provisional Patent Application No. 60/269,387, filed February 20, 2001, the contents of which are hereby incorporated herein by reference in their entirety.

FIELD OF THE INVENTION

The present invention relates generally to the field of electronic or computerized commerce systems. Specifically, the present invention deals with anonymous transactions between a customer and a vendor.

BACKGROUND OF THE INVENTION

Systems for the purchase, usage, distribution and monitoring of digital content over the Internet have existed for some time. The majority of these systems are aimed at supplying consumers with the ability to shop for digital content on-line. The systems are usually designed in client-server methodology; hence, a consumer uses client software to engage in a buying session with the server, which later shall deliver the content to the consumer. The most common payment method is based on credit cards, and therefore requires the personal details of the consumer. In this case, the client-server interaction is also used to transfer the consumer details needed for the monetary transaction, such as name, billing address, mailing address, credit card number, telephone numbers, social security ID number and more. Those personal details are stored in the server's database for billing and customer care.

Such method risk the consumers privacy, since:

1) The high number of such systems increases the likelihood that individuals may gain illegal and /or unauthorized access to at least one of these systems and make harmful and /or undesirable use of the information.

2) System users can track the preferences of their individual clients.

Methods for anonymous purchases using computer networks exist. Some of these methods are based on pre-paid, "digital cash". Those methods are, in general cumbersome and have not acquired much popularity. Methods that provide anonymous payments using credit cards also exist. In general, these methods are based on separating the order information (OI) from the payment instruction (PI), by introducing another entity, generally referred to as "acquirer", that guarantees, from behalf of the user, that the payment instruction are indeed valid without revealing the actual details of the user, so that the payment protocol provides the vendor only the order information such as the purchased items and their respective sales price, and the acquirer only with the credit-card information, so that the vendor is not required to have an access to the customer's credit card information, as long as the acquirer authorizes the purchase. This separation is achieved using either cryptographic methods or by deploying at least two paths (customer-vendor for order information, customer-acquirer for payment information and acquirer-vendor for authorization information). E.g., United States Patent 5,420,926 describes a method for anonymous credit card transactions. The techniques include the use of a communications exchange so that information and funds may be transferred without the destination for the transfer knowing the source of the information or funds and the use of public key encryption so that each party to the transaction and the communications exchange can read only the information the party or the exchange needs for its role in the transaction. United States Patent 6,119,101 describes a system for electronic commerce having personal agents that conceal the identity of the consumer. United States Patent 6,108,644 describes a system and method for electronic transactions, including registration, audit and trusted recovery features, whereas transaction request message is received from a registered user that includes an unblinded validated certificate, and a blinded unvalidated certificate. If the unblinded validated certificate is determined to be legitimate, then a transaction can be performed, and the blinded unvalidated certificate is validated to obtain a blinded, validated certificate that is sent to the user.

While these methods provide an adequate level of anonymity in the buying

phase, there is still a need to establish an initial connection between the client and the vendor, and the digital and/or physical goods need to be sent, eventually, to the customer by the vendor. Using current methods usually requires that in order to create this connection, both parties to the connection disclose information regarding their identity. Thus, current methods do not provide an adequate level of anonymity in these phases, and unauthorized individuals or organization taking advantage of the pitfalls of current methods may violate the anonymity of consumers.

SUMMARY OF THE INVENTION

The present invention seeks to provide a novel method to facilitate fully anonymous purchases. Specifically, the current invention provides methods that allow anonymous distribution and delivery of digital and/or physical entities, thereby allowing the buyer to remain anonymous throughout the entire buying process.

In a preferred embodiment of the present invention the anonymization method utilizes an anonymous initial connection between the vendor and the client and an anonymous distribution and delivery route, based on a chain of three or more consecutive entities, the first of them is the source of the item to be sent, and the last of them is the final client. The full address of the client is sent only to the one-before-last entity in the chain, together with an index that is unique to the special transaction. The other entities in the chain are supplied only with the transaction index. In cases where there are only three entities, the source does not know the details of the client, and the middle entity does not know the details of the purchased items. However, using this method, the middle entity is still aware of both the source and the client addresses. In order to elevate the anonymity level, in a preferred embodiment of the present invention, another entity is placed between the source and the next-to the client entity, thereby enabling the masking of the identity of the source from the next-to-the client entity.

According to a first aspect of the present invention there is provided a method for making an anonymous computerized commerce transaction involving the delivery of digital merchandise comprising the steps of sending first sensitive information from a first

entity to a first intermediate entity; processing said first sensitive information by said first intermediate entity; creating first non sensitive information operable to approve said transaction by said first intermediate entity; sending said first non sensitive information to a third entity operable to perform said transaction; performing said transaction by said third entity, and transferring said digital merchandise to said first entity via a delivering entity comprising information operable to deliver said digital merchandise to said first entity without revealing said first sensitive information to said third entity.

In a preferred embodiment of the present invention, the digital media content comprises digital video media content.

In a preferred embodiment of the present invention, the digital media content comprises digital audio media content.

In a preferred embodiment of the present invention, the digital merchandise comprises digital software.

In a preferred embodiment of the present invention, the method further comprises a second intermediate entity operable to receive second sensitive information from the third entity and operable to process the second sensitive information and operable to create second non sensitive information operable to be sent to the first entity without revealing the second sensitive information the second non sensitive information operable to approve the transaction.

In a preferred embodiment of the present invention, at least two intermediate entities of a substantially similar function to the second intermediate entity are used by the third entity in order to interact with at least two entities substantially similar to the first entity.

In a preferred embodiment of the present invention, at least one of the intermediate entities of a substantially similar function to the second intermediate entity comprises functionality to authenticate the third entity.

In a preferred embodiment of the present invention, the method further comprises performing the functionality of both the first intermediate entity and of the second intermediate entity by one entity.

In a preferred embodiment of the present invention, at least two intermediate entities of a substantially similar function to the first intermediate entity are used by the first entity in order to interact with at least two entities substantially similar to the third entity.

In a preferred embodiment of the present invention, at least one of the intermediate entities of a substantially similar function to the first intermediate entity comprises functionality to authenticate the first entity.

In a preferred embodiment of the present invention, the first sensitive information contains information operable to identify the first entity.

In a preferred embodiment of the present invention, the second sensitive information contains information operable to identify the third entity.

In a preferred embodiment of the present invention, the first sensitive information contains information operable to perform payment for the digital merchandise.

In a preferred embodiment of the present invention, the first intermediate entity comprises functionality to authenticate the first entity.

In a preferred embodiment of the present invention, the second intermediate entity comprises functionality to authenticate the third entity.

In a preferred embodiment of the present invention, the first intermediate entity is operable to perform payment for the digital merchandise.

In a preferred embodiment of the present invention, at least two intermediate entities of a substantially similar function to the first intermediate entity are used by the first entity in order to interact with the third entity.

In a preferred embodiment of the present invention, at least two intermediate entities of a substantially similar function to the second intermediate entity are used by the third entity in order to interact with the first entity.

In a preferred embodiment of the present invention, at least one of the intermediate entities of a substantially similar function to the first intermediate entity comprises functionality to authenticate the first entity.

In a preferred embodiment of the present invention, at least one of the intermediate entities of a substantially similar function to the second intermediate entity

comprises functionality to authenticate the third entity.

In a preferred embodiment of the present invention, at least one of the intermediate entities of a substantially similar function to the first intermediate entity is operable to perform payment for the digital merchandise.

In a preferred embodiment of the present invention, at least one of the intermediate entities of a substantially similar function to the first intermediate entity is operable to perform payment for the digital merchandise.

In a preferred embodiment of the present invention, the method further comprises a third intermediate entity operable to receive third sensitive information from the third entity and operable to process the second sensitive information and operable to create third non sensitive information operable to be sent to a fourth entity without revealing the third sensitive information, the third non sensitive information operable to approve the transaction.

In a preferred embodiment of the present invention, at least two intermediate entities of a substantially similar function to the third intermediate entity are used by the third entity in order to interact with at least two entities substantially similar to the fourth entity.

In a preferred embodiment of the present invention, at least two intermediate entities of a substantially similar function to the third intermediate entity are used by the third entity in order to interact with the fourth entity.

In a preferred embodiment of the present invention, at least one of the intermediate entities of a substantially similar function to the third intermediate entity comprises functionality to authenticate the third entity.

In a preferred embodiment of the present invention, at least one of the intermediate entities of a substantially similar function to the third intermediate entity comprises functionality to authenticate the third entity.

In a preferred embodiment of the present invention, the third sensitive information contains information operable to identify the third entity.

In a preferred embodiment of the present invention, the method further

comprises performing the functionality of both the first intermediate entity and of the third intermediate entity by one entity.

In a preferred embodiment of the present invention, the method further comprises utilizing a coordinating entity, the coordinating entity comprises functionality to store coordinating information operable to direct the first entity to utilize the first intermediate entity in order to perform the transaction with the third entity without the need for the first entity to be aware of the identity of the third entity.

In a preferred embodiment of the present invention, the first entity comprises functionality to store the coordinating information on the coordinating entity.

In a preferred embodiment of the present invention, the third entity comprises functionality to store the coordinating information on the coordinating entity.

In a preferred embodiment of the present invention, the functionality to store the coordinating information on the coordinating entity comprises utilizing a fourth intermediate entity operable to store the coordinating information on the coordinating entity without revealing identifying information of the first entity to the coordinating entity.

In a preferred embodiment of the present invention, the functionality to store the coordinating information on the coordinating entity comprises utilizing a fifth intermediate entity operable to store the coordinating information on the coordinating entity without revealing identifying information of the third entity to the coordinating entity.

In a preferred embodiment of the present invention, the method further comprises utilizing a coordinating entity, the coordinating entity comprises functionality to store coordinating information operable to direct the first entity to utilize the first intermediate entity in order to perform the transaction with the third entity without the need for the first entity to be aware of the identity of the third entity.

In a preferred embodiment of the present invention, the first entity comprises functionality to store the coordinating information on the coordinating entity.

In a preferred embodiment of the present invention, the third entity comprises functionality to store the coordinating information on the coordinating entity.

In a preferred embodiment of the present invention, the functionality to store the

coordinating information on the coordinating entity comprises utilizing a fourth intermediate entity operable to store the coordinating information on the coordinating entity without revealing identifying information of the first entity to the coordinating entity.

In a preferred embodiment of the present invention, the functionality to store the coordinating information on the coordinating entity comprises utilizing a fifth intermediate entity operable to store the coordinating information on the coordinating entity without revealing identifying information of the third entity to the coordinating entity.

In a preferred embodiment of the present invention, the information operable to direct the first entity to utilize the first intermediate entity in order to perform the transaction with the third entity without the need for the first entity to be aware of the identity of the third entity comprises information operable to enable the first entity to direct the first intermediate entity to contact the second intermediate entity and to direct the second intermediate entity to perform the following actions: contact the third intermediate entity and to initiate the transaction.

In a preferred embodiment of the present invention, some of the communication of information communicated between two entities in the course of executing and approving the transaction comprise of sending the communication via an entity which is not a party to the communication of information communicated between two entities in the course of executing and approving the transaction.

In a preferred embodiment of the present invention, the entity which is not a party to the communication of information communicated between two entities in the course of executing and approving the transaction is a party to other communication with the two entities thereby eliminating one of the communication channels needed to execute and approve the transaction.

In a preferred embodiment of the present invention, the communication sent via an entity which is not a party to the communication of information communicated between two entities in the course of executing and approving the transaction comprises protection against forgery by a signature thereby preventing the entity which is not a party to the communication of information communicated between two entities in the course of

executing and approving the transaction from forging information.

In a preferred embodiment of the present invention, the communication sent via an entity which is not a party to the communication of information communicated between two entities in the course of executing and approving the transaction comprises protection against forgery by encryption thereby preventing the entity which is not a party to the communication of information communicated between two entities in the course of executing and approving the transaction from accessing the communication sent via an entity which is not a party to the communication of information communicated between two entities in the course of executing and approving the transaction.

In a preferred embodiment of the present invention, the technique of sending the communication via an entity which is not a party to the communication of information communicated between two entities in the course of executing and approving the transaction is used to transform sensitive information into non sensitive information by preventing the transfer of sensitive information that would result by direct communication by the two entities.

In a preferred embodiment of the present invention, the eliminated sensitive information whose transfer would result from direct communication by the two entities comprises information about the identity of at least one of the two entities.

In a preferred embodiment of the present invention, the eliminated sensitive information whose transfer would result from direct communication by the two entities comprises information about the address of at least one of the two entities.

In a preferred embodiment of the present invention, the signature is a cryptographic signature.

In a preferred embodiment of the present invention, the digital merchandise comprises encrypted content.

In a preferred embodiment of the present invention, the encrypted content is transferred to the first entity separately from the encrypted content's decryption key.

In a preferred embodiment of the present invention, the method further comprises a third intermediate entity operable to receive third sensitive information from

the third entity and operable to process the second sensitive information and operable to create third non sensitive information operable to be sent to a fourth entity without revealing the third sensitive information the third non sensitive information operable to approve the transaction and the method further comprises performing the functionality of at least two of the following by one entity: of the first intermediate entity, of the second intermediate entity and of the third intermediate entity.

In a preferred embodiment of the present invention, at least two intermediate entities of a substantially similar function to the third intermediate entity are used by the third entity in order to interact with at least two entities substantially similar to the fourth entity.

In a preferred embodiment of the present invention, at least two intermediate entities of a substantially similar function to the third intermediate entity are used by the third entity in order to interact with the fourth entity.

In a preferred embodiment of the present invention, at least one of the intermediate entities of a substantially similar function to the third intermediate entity comprises functionality to authenticate the third entity.

In a preferred embodiment of the present invention, at least one of the intermediate entities of a substantially similar function to the third intermediate entity comprises functionality to authenticate the third entity.

In a preferred embodiment of the present invention, the third sensitive information contains information operable to identify the third entity.

In a preferred embodiment of the present invention, the method further comprises performing the functionality of both the first intermediate entity and of the coordinating entity by one entity.

In a preferred embodiment of the present invention, the method further comprises performing the functionality of at least two of the following by one entity: of the first intermediate entity, of the fourth intermediate entity and of the coordinating entity.

In a preferred embodiment of the present invention, the method further comprises performing the functionality of at least two of the following by one entity: of the

first intermediate entity, of the second intermediate entity and of the coordinating entity.

In a preferred embodiment of the present invention, the method further comprises performing the functionality of at least two of the following by one entity: of the first intermediate entity, of the second intermediate entity, of the fourth intermediate and of the coordinating entity.

In a preferred embodiment of the present invention, the method further comprises performing the functionality of at least two of the following by one entity: of the first intermediate entity, of the second intermediate entity, of the fifth intermediate and of the coordinating entity.

In a preferred embodiment of the present invention, the third entity comprises functionality to store the coordinating information on the coordinating entity and the functionality to store the coordinating information on the coordinating entity comprises utilizing a fifth intermediate entity operable to store the coordinating information on the coordinating entity without revealing identifying information of the third entity to the coordinating entity and the method further comprises performing the functionality of at least two of the following by one entity: of the first intermediate entity, of the second intermediate entity, of the fourth intermediate, of the fifth intermediate and of the coordinating entity.

In a preferred embodiment of the present invention, the method further comprises a third intermediate entity operable to receive third sensitive information from the third entity and operable to process the second sensitive information and operable to create third non sensitive information operable to be sent to a fourth entity without revealing the third sensitive information, the third non sensitive information operable to approve the transaction and the method further comprises performing the functionality of at least two of the following by one entity: of the first intermediate entity, of the coordinating entity and of the third intermediate entity.

In a preferred embodiment of the present invention, at least two intermediate entities of a substantially similar function to the third intermediate entity are used by the third entity in order to interact with at least two entities substantially similar to the fourth

entity.

In a preferred embodiment of the present invention, at least two intermediate entities of a substantially similar function to the third intermediate entity are used by the third entity in order to interact with the fourth entity.

In a preferred embodiment of the present invention, at least one of the intermediate entities of a substantially similar function to the third intermediate entity comprises functionality to authenticate the third entity.

In a preferred embodiment of the present invention, at least one of the intermediate entities of a substantially similar function to the third intermediate entity comprises functionality to authenticate the third entity.

In a preferred embodiment of the present invention, the third sensitive information contains information operable to identify the third entity.

In a preferred embodiment of the present invention, the method further comprises a third intermediate entity operable to receive third sensitive information from the third entity and operable to process the second sensitive information and operable to create third non sensitive information operable to be sent to a fourth entity without revealing the third sensitive information, the third non sensitive information operable to approve the transaction and the method further comprises performing the functionality of at least two of the following by one entity: of the first intermediate entity, of the second intermediate entity, of the coordinating entity and of the third intermediate entity.

In a preferred embodiment of the present invention, at least two intermediate entities of a substantially similar function to the third intermediate entity are used by the third entity in order to interact with at least two entities substantially similar to the fourth entity.

In a preferred embodiment of the present invention, at least two intermediate entities of a substantially similar function to the third intermediate entity are used by the third entity in order to interact with the fourth entity.

In a preferred embodiment of the present invention, at least one of the intermediate entities of a substantially similar function to the third intermediate entity

comprises functionality to authenticate the third entity.

In a preferred embodiment of the present invention, at least one of the intermediate entities of a substantially similar function to the third intermediate entity comprises functionality to authenticate the third entity.

In a preferred embodiment of the present invention, the third sensitive information contains information operable to identify the third entity.

In a preferred embodiment of the present invention, the method further comprises a third intermediate entity operable to receive third sensitive information from the third entity and operable to process the second sensitive information and operable to create third non sensitive information operable to be sent to a fourth entity without revealing the third sensitive information, the third non sensitive information operable to approve the transaction and the method further comprises performing the functionality of at least two of the following by one entity: of the first intermediate entity, of the fourth intermediate entity, of the coordinating entity and of the third intermediate entity.

In a preferred embodiment of the present invention, at least two intermediate entities of a substantially similar function to the third intermediate entity are used by the third entity in order to interact with at least two entities substantially similar to the fourth entity.

In a preferred embodiment of the present invention, at least two intermediate entities of a substantially similar function to the third intermediate entity are used by the third entity in order to interact with the fourth entity.

In a preferred embodiment of the present invention, at least one of the intermediate entities of a substantially similar function to the third intermediate entity comprises functionality to authenticate the third entity.

In a preferred embodiment of the present invention, at least one of the intermediate entities of a substantially similar function to the third intermediate entity comprises functionality to authenticate the third entity.

In a preferred embodiment of the present invention, the third sensitive information contains information operable to identify the third entity.

In a preferred embodiment of the present invention, the method further comprises a third intermediate entity operable to receive third sensitive information from the third entity and operable to process the second sensitive information and operable to create third non sensitive information operable to be sent to a fourth entity without revealing the third sensitive information, the third non sensitive information operable to approve the transaction and the method further comprises performing the functionality of at least two of the following by one entity: of the first intermediate entity, of the second intermediate entity, of the fourth intermediate entity, of the coordinating entity and of the third intermediate entity.

In a preferred embodiment of the present invention, at least two intermediate entities of a substantially similar function to the third intermediate entity are used by the third entity in order to interact with at least two entities substantially similar to the fourth entity.

In a preferred embodiment of the present invention, at least two intermediate entities of a substantially similar function to the third intermediate entity are used by the third entity in order to interact with the fourth entity.

In a preferred embodiment of the present invention, at least one of the intermediate entities of a substantially similar function to the third intermediate entity comprises functionality to authenticate the third entity.

In a preferred embodiment of the present invention, at least one of the intermediate entities of a substantially similar function to the third intermediate entity comprises functionality to authenticate the third entity.

In a preferred embodiment of the present invention, the third sensitive information contains information operable to identify the third entity.

In a preferred embodiment of the present invention, the method further comprises a third intermediate entity operable to receive third sensitive information from the third entity and operable to process the second sensitive information and operable to create third non sensitive information operable to be sent to a fourth entity without revealing the third sensitive information, the third non sensitive information operable to

approve the transaction and the method further comprises performing the functionality of at least two of the following by one entity: of the first intermediate entity, of the second intermediate entity, of the fifth intermediate entity, of the coordinating entity and of the third intermediate entity.

In a preferred embodiment of the present invention, at least two intermediate entities of a substantially similar function to the third intermediate entity are used by the third entity in order to interact with at least two entities substantially similar to the fourth entity.

In a preferred embodiment of the present invention, at least two intermediate entities of a substantially similar function to the third intermediate entity are used by the third entity in order to interact with the fourth entity.

In a preferred embodiment of the present invention, at least one of the intermediate entities of a substantially similar function to the third intermediate entity comprises functionality to authenticate the third entity.

In a preferred embodiment of the present invention, at least one of the intermediate entities of a substantially similar function to the third intermediate entity comprises functionality to authenticate the third entity.

In a preferred embodiment of the present invention, the third sensitive information contains information operable to identify the third entity.

In a preferred embodiment of the present invention, the third entity comprises functionality to store the coordinating information on the coordinating entity and the functionality to store the coordinating information on the coordinating entity comprises utilizing a fifth intermediate entity operable to store the coordinating information on the coordinating entity without revealing identifying information of the third entity to the coordinating entity and the method further comprises a third intermediate entity operable to receive third sensitive information from the third entity and operable to process the second sensitive information and operable to create third non sensitive information operable to be sent to a fourth entity without revealing the third sensitive information, the third non sensitive information operable to approve the transaction and the method further comprises

performing the functionality of at least two of the following by one entity: of the first intermediate entity, of the second intermediate entity, of the third intermediate entity, of the fourth intermediate, of the fifth intermediate and of the coordinating entity.

In a preferred embodiment of the present invention, at least two intermediate entities of a substantially similar function to the third intermediate entity are used by the third entity in order to interact with at least two entities substantially similar to the fourth entity.

In a preferred embodiment of the present invention, at least two intermediate entities of a substantially similar function to the third intermediate entity are used by the third entity in order to interact with the fourth entity.

In a preferred embodiment of the present invention, at least one of the intermediate entities of a substantially similar function to the third intermediate entity comprises functionality to authenticate the third entity.

In a preferred embodiment of the present invention, at least one of the intermediate entities of a substantially similar function to the third intermediate entity comprises functionality to authenticate the third entity.

In a preferred embodiment of the present invention, the third sensitive information contains information operable to identify the third entity.

In a preferred embodiment of the present invention, the method further comprising communicating at least some of the information communicated in the course of approving and executing the transaction via a least one intermediate entity.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be understood and appreciated more fully from the following detailed description taken in conjunction with the appended drawings in which:

Fig. 1 is a simplified conceptual illustration of a system for anonymous commerce, constructed and operative in accordance with a preferred embodiment of the present invention;

Fig. 2 is an illustration of a system, substantially similar to the system of figure

1, constructed and operative in accordance with a preferred embodiment of the present invention, where another anonymous delivery service is added to the system;

Fig. 3 is an illustration of a system, substantially similar to the system of figure 1, and figure 2, constructed and operative in accordance with a preferred embodiment of the present invention, where another anonymity service is introduced in the monetary transaction route;

Fig. 4 illustrates a system, similar to the systems in figures 1-3, that is used for anonymous delivery of encrypted digital content;

Fig. 5 illustrates a method, operative in accordance with a preferred embodiment of the present invention, that allows to establish anonymous connection between the vendor and a client, and

Fig. 6 illustrates a method, operative in accordance with a preferred embodiment of the present invention, that further enhance the anonymity level by introducing an acquirer buffer.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

The present invention seeks to provide a system and a method for anonymous transactions. For a better understanding of the invention and to show how the same may be carried into effect, reference will now be made, purely by way of example, to the accompanying drawings.

With specific reference now to the drawings in detail, it is stressed that the particulars shown are by way of example and for purposes of illustrative discussion of the preferred embodiments of the present invention only, and are presented in the cause of providing what is believed to be the most useful and readily understood description of the principles and conceptual aspects of the invention. In this regard, no attempt is made to show structural details of the invention in more detail than is necessary for a fundamental understanding of the invention, the description taken with the drawings making apparent to those skilled in the art how at least two forms of the invention may be embodied in practice.

Turning now to figure 1, there is illustrated a simplified block conceptual

illustration of a system for anonymous commerce, constructed and operative in accordance with a preferred embodiment of the present invention, in which a client 110 sends a request to a vendor 130 that contains order information 112. In a preferred embodiment of the present invention, the client utilizes a standard anonymizing service 120, which is preferably provided by at least two internet sites in order to mask the client internet protocol (IP) address from the vendor, thereby further enhancing the level of anonymity. The client 110 in turn receives from the vendor 130 the transaction identification number (ID) 114 via the same route. This transaction number is preferably a globally unique variable that is shared between various entities in the system, and may be created by any of the entities or by utilizing at least two of them, preferably being created by the vendor. The client sends the payment instruction (PI) 116, which may include the amount to be paid, terms of payment, relevant details of the vendor etc, preferably encrypted and certificated, together with the transaction ID 114, to the acquirer 140, which approves and guarantees the transaction (e.g., by performing a credit-card clearance). The acquirer then sends the vendor 130 the transaction ID 114 together with payment approval 142 to the vendor 130, thereby allowing the vendor 130 to approve the transaction 132. The transaction approval may be performed between the vendor 130 and the acquirer 140, the vendor and a 3rd party, or by another known method. The client also sends his address and/or other delivery information 118 to the anonymous delivery service 150, together with the transaction ID 114, and in turn receives the ID 152 of the anonymous delivery service 150, which he sends to the vendor 130. After the approval of the transaction, the vendor sends the virtual and/or physical purchased item 136 to the anonymous delivery service 150, together with the transaction ID 114. The anonymous delivery service associates the transaction ID to the client address and/or other delivery information and sends the item 132 to the client 110.

In a preferred embodiment of the present invention, all the operations are automatically preformed by computer programs in the various entities.

In order to illustrate the above method, consider the following scenario: the client, Mrs. Jane Doe, wishes to buy astronomical software from the Internet site astrodoe.com. She uses her web browser in order to connect to the anonymization site

anonydoe.net, and keep browsing with her IP masked by the site software. She orders the software and a software client on her computer gets the corresponding transaction ID 114 from the vendor via the anonimyzer. The software client then sends the payment instruction (PI), (e.g., credit-card details, the amount of money, the number of payments etc...), together with the transaction ID to the acquirer 140, and delivery information (e.g., physical and/or e-mail address and/or IP address) to the anonymous delivery service. The acquirer confirms that the credit card is valid, and preferably also authenticates the client, in order to reduce the chances for fraud. The acquirer then sends the vendor the approval to the transaction 142, using the transaction ID 114 in order to identify the transaction. The vendor then sends the acquirer the approval for the transaction, and sends the software, wrapped in a manner that does not conceal its content to the anonymous delivery service 150, together with the corresponding transaction ID. The anonymous delivery service 150 completes the transaction by sending the software to Mrs. Jane Doe. Using this methods, none of the entities involved in the transaction is exposed both to the content of the purchased item and the identity of the customer.

Using the above method, the anonymous delivery service 150 still has transport information, i.e., the fact that a certain client bought something from a certain vendor. This problem can be solved by introducing another anonymous delivery service: turning now to figure 2, there is illustrated a method, substantially similar to the method of figure 1, constructed and operative in accordance with a preferred embodiment of the present invention, where another anonymous delivery service 255 is added to the system. (for brevity, the first digit of the numbers in the drawing is equal to the figure number, while the other digits remain consistent between the substantially similar entities in the various drawing). Here, again, the client 210 uses the anonymizer 220 to send a request to the vendor 230 that contained the order information 212 and gets back the transaction ID 214. The client sends the payment instruction (PI) 216, together with the transaction ID 214, to the acquirer 240. The acquirer then sends the transaction ID 214 together with payment approval 242 to the vendor 230. The client also sends his address and / or other delivery information 218 to the first anonymous delivery service 250, together with the transaction

ID 214 and gets back the ID 252 of the first anonymous delivery service 250, which he sends to the vendor 230. After the approval of the transaction, the vendor sends the virtual and/or physical purchased item 236 to the second anonymous delivery service 250, together with the transaction ID 214. The second anonymous delivery service 255 associates the transaction ID 214 with the ID 252 of the first anonymous delivery service 250, and sends the purchases item 232, together with the transaction ID 214 to the first anonymous delivery service 250. The first anonymous delivery service associates the transaction ID to the client address and / or other delivery information and sends the item 232 to the client 210. Information regarding the identity of the vendor is known only to the second anonymous delivery service 255, which receives items from at least two vendors 234, while information regarding the identity of the client is known only to anonymous delivery service 250.

The above scheme for obscuring the transport details may also be used in order to obscure the details of the monetary transaction: turning now to figure 3, there is illustrated a method, substantially similar to the methods of figures 1 and 2, constructed and operative in accordance with a preferred embodiment of the present invention, where another anonymity service 345 is introduced in order to mask some of the details of the monetary transaction. Information regarding the identity of the vendor is known only to the anonymous service 345, that preferably form connections with at least two vendors 334, while information regarding the identity of the client is known only to the acquirer 340, which preferably form connections with at least two clients 315. Here, again, the client 310 uses the anonymizer 320 to send a request to the vendor 330 that contained the order information 312 and get back the transaction ID 314. The client sends the payment instruction (PI) 316, together with the transaction ID 314, to the acquirer 340. The acquirer then sends an acquirer ID 331 to the client 310, who sends the acquirer ID 331 to the vendor. The vendor then sends the acquirer ID 331 to the monetary transport anonymizer 345. The acquirer sends the transaction ID 314 together with payment approval 342 to the monetary transport anonymizer 345. The client 310 also sends his address and / or other delivery information 318 to the first anonymous delivery service 350, together with the transaction ID 314 and gets back the ID 352 of the first anonymous delivery service 350,

which he sends to the vendor 330. After the approval of the transaction, the vendor sends the digital and/or physical purchased item 336 to the second anonymous delivery service 355, together with the transaction ID 314. The second anonymous delivery service associates the transaction ID 314 to the ID 352 of the first anonymous delivery service 350, and sends the purchases item 336, together with the transaction ID 314 to the first anonymous delivery service 350. The first anonymous delivery service associates the transaction ID to the client address and / or other delivery information and sends the item 332 to the client 310.

The anonymous delivery service described above can be used for the distribution of both physical and digital content. For the anonymous delivery of physical content, the vendor should wrap the items in a case or an envelope that may contain the transaction ID, or the transaction ID may be linked to the physical content in some other way. The anonymous delivery service may transform this ID (or part of it) to the address or to the delivery information of the client. For anonymous delivery of digital content, the role of the envelope may be taken by encryption and / or other means. The key for the decryption of the content may be sent to the client using the same anonymous route that the client used in order to send the vendor his order information and transaction ID. Figure 4 illustrates a method, constructed and operative in accordance with a preferred embodiment of the present invention, which is substantially similar to the one described in figures 1-3, but the acquirer now sends the client an encrypted digital content: The client 410 uses the anonymizer 420 to send a request to the vendor 430 that contained the order information 412 and get back the transaction ID 414 and an encryption key 438. The client sends the payment instruction (PI) 416, together with the transaction ID 414, to the acquirer 440. The acquirer then sends an acquirer ID 431 to the client 410, who sends the acquirer ID 431 to the vendor. The vendor then sends the acquirer ID 431 to the monetary transport anonimizer 445. The acquirer sends the transaction ID 414 together with payment approval 442 to the monetary transport anonymizer 445. The client 410 also sends his delivery information 418 to the first anonymous delivery service 450, together with the transaction ID 414 and gets back the ID 452 of the first anonymous delivery service 450, which the client 410 sends to

the vendor 430. After the approval of the transaction, the vendor sends the purchased digital item 436, encrypted using the key 438, to the second anonymous delivery service 450, together with the transaction ID 414. The second anonymous delivery service associates the transaction ID 414 to the ID 452 of first anonymous delivery service 450, and sends the purchases item 432, together with the transaction ID 414 to the first anonymous delivery service 450. The first anonymous delivery service associates the transaction ID to the client address and / or other delivery information and sends the item 432 to the client 410, which decrypt the encrypted content 436 using the key 438.

Turning now to figure 5, there is illustrated a method, operative in accordance with a preferred embodiment of the present invention, that allows to establish anonymous connection between the vendor and a client, in a manner that assures that no single entity is exposed to the identity of both sides of the transaction: The vendor 530 publish the goods it offers 533 in the arena 560 using the anonimizer 525, which is preferably also connected to other vendors 534. The goods are published together with the address 527 of the anonymizer 525 (the address may be its Internet protocol (IP) address). The client 510 uses the anonimizer 520, which is preferably connected to other clients 515, in order to look for items that are offered in the arena 560. If the client is interested in buying the goods 533, it uses the address 527 in order to establish a connection with vendor 530 via the anonymizer 525. Using this method, no single entity is aware of the identity of the both sides of the transaction.

Reference is now made to figure 6, which illustrates a method, operative in accordance with a preferred embodiment of the present invention, that further enhance the anonymity level by introducing an acquirer buffer, to which at least two clients are connected, and is used to mask some of the information regarding the clients (e.g., its Internet protocol (IP) address): the client 610 uses the anonymizer 620 to send a request to the vendor 630 that contained the order information 612 and get back the transaction ID 614. The client sends the payment instruction (PI) 616, together with the transaction ID 614 to the acquirer buffer 643. The client may also send the acquirer buffer 643 additional information 617 that may be used for authentication or as a proof that the client is eligible

to perform the transaction. The acquirer buffer 643 sends the payment instruction (PI) 616 together with the transaction ID 614 and preferably also the additional information 617 to the acquirer 640. The acquirer checks that the payment instruction (PI) 616 is valid and then sends an acquirer ID 631 to the client 610, who sends the acquirer ID 631 to the vendor. The vendor then sends the acquirer ID 631 to the monetary transport anonimizer 645. The acquirer sends the transaction ID 614 together with payment approval 642 to the monetary transport anonymizer 645, which then sends the transaction ID 614 together with payment approval 642 to the vendor 630. The client 610 also sends its delivery information 618 to the first anonymous delivery service 650, together with the transaction ID 614, and gets back the ID 652 of the first anonymous delivery service 650, which the client 610 sends to the vendor 630. After the approval of the transaction, the vendor sends the purchased digital item 636, encrypted with the key 638, to the second anonymous delivery service 650, together with the transaction ID 614. The second anonymous delivery service associates the transaction ID 614 to the ID 652 of first anonymous delivery service 650, and sends the purchases item 632, together with the transaction ID 614 to the first anonymous delivery service 650. The first anonymous delivery service associates the transaction ID to the client address and / or other delivery information and sends the item 632 to the client 610, which decrypt the encrypted content 636 using the key 638.

In a preferred embodiment of the present invention, a coordinating entity exist to enable a client to chose a vendor without being aware of the identity of the vendor, the vendor is registered, preferably via an anonymizer into the coordinating entity's database, the information registered is preferably validated or otherwise vouched for, afterward (or, in case of a similarily registered client, possibly beforehand) the client contacts the coordinating entity and ask for a vendor which can supply the desired merchandise to the client in agreeable terms, preferably selecting the most suitable vendor, the coordinating entity supplies the client with the needed details to contact the vendor without revealing who is the vendor (e.g. the vendor's anonimizer's address).

It is appreciated that one or more steps of any of the methods described herein may be implemented in a different order than that shown, while not departing from the

spirit and scope of the invention.

While the present invention may or may not have been described with reference to specific hardware or software, the present invention has been described in a manner sufficient to enable persons having ordinary skill in the art to readily adapt commercially available hardware and software as may be needed to reduce any of the embodiments of the present invention to practice without undue experimentation and using conventional techniques.

While the present invention has been described with reference to one or more specific embodiments, the description is intended to be illustrative of the invention as a whole and is not to be construed as limiting the invention to the embodiments shown. It is appreciated that various modifications may occur to those skilled in the art that, while not specifically shown herein, are nevertheless within the true spirit and scope of the invention.